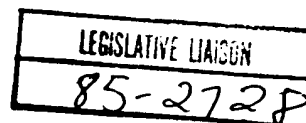




EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 17, 1985
LEGISLATIVE REFERRAL MEMORANDUM



TO:

Department of Defense - Werner Windus (697-1305)

General Services Administration - Ted Ebert (566-1250)

✓ Central Intelligence Agency

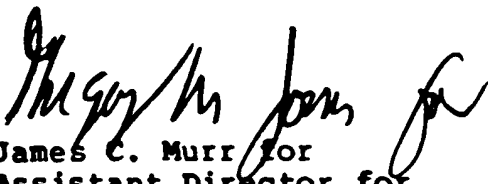
SUBJECT: Commerce (NBS) testimony on H.R. 2889, the "Computer Security Research and Training Act of 1985."

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with Circular A-19.

Please provide us with your views no later than

2:30 P.M. TODAY, SEPTEMBER 17, 1985

Direct your questions to Gregory Jones (395-3454), of this office.


James C. Murr for
Assistant Director for
Legislative Reference

Enclosures

cc: S. Dotson
K. Sheid
E. Springer

70: GREG JONES

13454

7020

U.S. DEPARTMENT OF COMMERCE**STATEMENT OF MR. JAMES H. BURROWS****DIRECTOR, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY****NATIONAL BUREAU OF STANDARDS****BEFORE THE SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY****COMMITTEE ON GOVERNMENT OPERATIONS****U.S. HOUSE OF REPRESENTATIVES****SEPTEMBER 18, 1985****MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:**

Thank you for inviting me to speak to you today and for your interest in this critically important subject. The need for computer security has never been greater than it is today. The legislation that you are considering, HR 2889, takes note of the factors that contribute to this pressing need -- the government's dependence on computers, the scale of government computer operations, the widespread dispersal of personal computers throughout the government, and the valuable and sensitive information that is contained in government computer systems.

Rapidly changing technology and the escalating use of computers will continue to make computer security a high priority issue in the future. We see that it is impossible to return to manual methods once an organization adopts automated data processing methods. To achieve efficient information interchange, we must strive for standard, interchangeable hardware and software systems. At the same time, however, we will increase the vulnerability of our systems to external and internal threats.

09/17/85

09:15

EPT COMMERCE

NO. 003

001

To prevent serious accidents that cripple our ability to carry out data processing operations and to avoid compromise of sensitive information, we must stimulate an awareness for the need for computer security in managers and users of computer systems. This is the key element in a campaign to improve computer security, and this is the thrust of HR 2889. I believe that this legislation addresses clearly established needs for computer security research and for training the people who manage, use, and operate Federal government computers.

Training for computer security is going to be essential in tomorrow's computing environment. The reports last week about the high level of personal computer use in Federal agencies highlight the urgency of this need. Issuing directives to improve security will not be enough.

Structured, organized, systematic training opportunities will be a must if the Federal government expects to exploit the use of advanced technology for staff productivity and reduced costs of government.

The legislation calls for the National Bureau of Standards (NBS) to develop technical procedures and practices, and guidelines for use in training. Many guides and reports that NBS has developed are already available for use in training programs. However, in order to deal with the ~~computer security problem~~ as laid out in H.R. 2889, it will be necessary to expand ~~the kinds of materials~~ developed and to develop materials suitable for widely different needs. Computer security awareness programs must be available not only for the managers and users of automated information systems, but also for other agency personnel such as internal auditors, Inspectors General personnel, and budget analysts and managers. This

will be essential to enable corrective actions to be proposed and implemented for information system development, operation, and modification.

These awareness programs and the renewed emphasis on computer security will also heighten the demand for timely products from NBS. Further, as new uses are made of computers and as new users become familiar with computer capabilities, new weaknesses will be exposed. Therefore, continuing attention to research and the development of effective preventive techniques will be needed.

The Institute for Computer Sciences and Technology at the National Bureau of Standards is currently carrying out a ~~program~~ program of research in computer security areas. This program was started in 1972 as a component of our responsibilities under P.L. 89-306, the pioneering legislation authored by Chairman Brooks to improve the efficient and effective use of computers in the Federal government. Responsibility for developing computer security standards and guidelines is also specifically assigned to the Department of Commerce under OMB Circulars, and has been delegated to NBS.

The problems that we are addressing are broad in scope and include many different hazards -- for example, physical damage to computers, accidents, destruction of data, theft of data and software, programming and data errors, omissions, and abuse of computing resources. While breaking into systems and computer crime are serious incidents, they are just one aspect of the problem. We are also concerned about the losses that result from processing incorrect data, from interruptions to data processing, and from lack of controls to prevent misuse of computers by authorized personnel. A vast amount of unclassified, but sensitive, information must be protected.

This includes personal, proprietary, and other information protected under the Privacy and Freedom of Information Acts.

ICST's program is targetted to three principal objectives: computer integrity, this means the ability to prevent or detect unauthorized actions by systems or unauthorized modification of computer information; confidentiality, the ability to prevent unauthorized disclosure of information; and availability, the ability to assure that processing resources are ready and waiting when needed. Failure to achieve these objectives in Federal government computing operations could result in undesirable events ranging from threats to national security to denial of benefits to citizens, loss of Government money and resources, human injury, or loss of life.

Under our legislative charter and policy directives, we develop management guides, test methods, performance measures, technical information and advice, guidelines, and standards. In developing our products and services we pay particular attention to the problems of Federal computer users and to the development of cost effective security methods that are appropriate to the information and systems to be protected. We also emphasize good preventive techniques because it is more cost effective to avoid costly errors and accidents than to recoup after an expensive mistake. We have found that State and local governments, business, and industry users have problems similar to the Federal government's and that our technical products are used by the private sector as well as by the public sector. They are frequently used as the basis for training and education programs such as those conducted by the Small Business Administration and the Office of Personnel Management.

In the area of computer security and risk management, as well as in other program areas, we work closely with users in large and small organizations to learn about their experiences and their needs for technical and management solutions to their computer utilization problems. Because we are a small organization, we believe that the best way to achieve change is to work through ^{other} the organizations. We sponsor, and participate in, conferences, workshops, and meetings to share information and to keep users and industry informed of our activities, as well as to learn what others are doing. We respond to requests for advice and consultation, we participate in training seminars to the extent that we can, and we provide direct technical assistance to Federal agencies on a reimbursable basis for limited number of projects that are related to our program.

I want to emphasize especially our work with the Department of Defense and especially the DOD Computer Security Center. DOD has conducted extensive research in the development of security technology for national defense applications. We are continually evaluating the applicability of DOD's research activities to the civilian side of government and the private sector, so that we can transfer appropriate technology to the users who need it. Guest workers from DOD are working with ICST staff, and we maintain close staff contact on technical issues. We will be hosting the seventh joint workshop on computer security with DOD later this month. The workshops have been well attended by both government and industry participants.

We have cooperated with the General Accounting Office in their reviews and evaluation of agency computer security and have provided briefings and seminars on computer security to many Federal and State government

organizations. We also participate in meetings sponsored by business and industry organizations to learn what they are doing and to make their good practices available to government users. Groups that we work with include EDP auditors, computer security professionals, internal auditors, universities, bankers, lawyers, and computer user groups.

As a result of our interactions with these groups, we are in a position to analyze user experiences and to identify best practices based on currently available technology. We have published a variety of reports, documents, guides, and studies conveying what we have learned, and we recommend sources of information and assistance. Through our contacts at many levels and with many organizations, we try to leverage our products so they reach a wide audience. For example, we are a clearinghouse of information that we have collected on computer security training opportunities, reading lists, and computer security services. This information is available electronically on a computer-based bulletin board.

We cooperate with business and industry to develop national and international consensus standards for computers and networks. We can do this effectively because of our knowledge of user and industry needs for standards and the position of trust that we have as objective participants in the standards process. Our goal is to stimulate the development of off-the-shelf commercial products that will expand choices, provide for interoperability of components and systems, and broaden opportunities for applications of new technology.

We are working with voluntary standards development groups sponsored by the American National Standards Institute, Institute of Electrical and Electronics Engineers, the International Organization for Standardization,

the American Bankers Association, and other national and international groups. We also participate with the National Communications Systems and the General Services Administration to develop Federal Standards for telecommunications.

Another important collaborative effort is our work with the Department of the Treasury to develop a policy to assure the integrity of electronic fund transfers. Last year Treasury issued a directive requiring the use of a voluntary standard for Financial Institution Message Authentication, to protect the billions of dollars that are transferred electronically every day. ICST was a major contributor to the standard, and to other voluntary standards developed for the private sector banking community.

The Treasury directive requires that all of its bureaus' EFT transactions be authenticated using ~~Data~~ Encryption techniques. Authentication is a process of coding and decoding significant phrases in a message to assure that it has been sent by an authorized party and has not been tampered with during transmission. ICST staff has been working with the voluntary standards community to draft a standard for protecting the secret keys that are used in coding and decoding messages. Automated key management techniques that were developed and patented by ICST staff are specified in this standard. Available on a license-free basis to organizations that want to use them, these techniques are being implemented in ICST's laboratory to help organizations test their products for compliance with the standard. A list of certified message authentication devices and techniques will be developed by Treasury with ICST and National Security Agency assistance.

ICST is working in conjunction with the National Security Agency (NSA) in developing proposed standards for data integrity and security in distributed computer networks. These efforts will focus on methods of securing data communications using data encryption techniques in a network of microcomputers. Commercially available software, protocols, and equipment will be used wherever possible. The network and primary security features will be unclassified, but will be designed to support more stringent security requirements for special applications.

Security of personal computers is currently under investigation. We recently issued a guide explaining security threats in the use of small computers and ways to reduce the risks. We are looking at a widerange of commercially available computer security devices for small systems to develop guidance for users on cost effective and secure equipment.

We are participating in a joint project with the President's Council on Integrity and Efficiency to develop criteria for auditors to use in establishing their work plans for auditing for security and controls throughout the life cycle of an automated information system. Specific guides and recommendations will be issued through this effort.

Security must be an integral part of overall systems planning. Therefore, we must be concerned about security in all of our technical activities, and we must address all aspects of computer system development and operations. This includes software systems, networks, storage media, and other hardware components. The weak link can appear anywhere in a complex system, and a comprehensive approach is needed to assure that strengths in one part of the system are not wiped out by weaknesses elsewhere.

03/17/85

09:20

PT COMMERCE

IND. 884

4-881

As you know the Department of Commerce is one of the members of the National Telecommunications and Information Systems Security Committee established under National Security Decision Directive 145, and we have been participating in the Subcommittee on Automated Information Systems Security. A major focus is the development of definitions of sensitive, but unclassified, government or government-derived information which has an impact on national security.

We believe that we can contribute to the implementation of NSDD 145 which complements, but does not substitute for, our work. We expect to continue to issue Federal Information Processing Standards for automated information processing security under our current authorities. Those that are appropriate for issuance under NSDD 145 will be submitted for processing under the procedures that are being developed by the National Telecommunications and Information Security Committee. For example, Federal Information Processing Standard 112, Password Usage, is the first approved FIPS that will also be processed under the Directive. Its intended use includes protecting passwords in both the classified and unclassified information environments. It incorporates guidance developed by DOD Computer Security Center to use password systems in national security computer systems. By using the NSDD 145 mechanism for disseminating documents such as this, we can help to avoid duplication of efforts and achieve effective dissemination of coherent, consistent information on computer security throughout the Federal government.

I thank the Committee for its interest in ICST's work, and I will be very happy to answer your questions.